USTIC-INFO 01/22. Recomendaciones de Seguridad de Adobe Acrobat Reader DC

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por Andalucía-CERT, informa de que el **CCN-CERT**, del Centro Criptológico Nacional, **ha elaborado un guía de buenas prácticas con recomendaciones de seguridad sobre Adobe Acrobat Reader DC.** Dado lo extendido de este software entre el parque de puestos de usuario corporativos, **os recomendamos encarecidamente su lectura y la aplicación de estas recomendaciones en aquellos equipos de vuestra competencia.**

Procedemos a trasladaros la información facilitada por el propio CCN-CERT:

"*El CCN-CERT, del Centro Criptológico Nacional (CCN), ha publicado un nuevo informe de Buenas Prácticas BP/16 sobre recomendaciones de seguridad de Adobe Acrobat Reader DC, con el objeto de aplicar medidas de seguridad de forma automatizada y desatendida sobre un software de visualización de ficheros PDF.*

Este documento establece un procedimiento para mejorar la seguridad y proteger Adobe Acrobat Reader DC para mitigar las posibles vulnerabilidades y los riesgos frente a los que pudiera estar expuesto.

A lo largo de 31 páginas, este documento detalla el objeto y alcance de la misma así como la instalación y bastionado de Adobe Reader DC pista continua en Windows con capítulos dedicados a la instalación del producto, cómo aplicar valores de seguridad, los valores de registro y cómo deshabilitar la tarea de actualización y el servicio "Adobearmservice".

Finalmente, este documento incluye un decálogo de recomendaciones de seguridad entre las que se encuentra el bloqueo de vínculos a internet en este tipo de documentos o la recomendación de no instalar plugins de terceros.

Para facilitar la aplicación del refuerzo de seguridad sobre Acrobat Reader DC, se incluye una carpeta de scripts que contiene los ficheros necesarios para el bastionado del programa.

El propósito de los scripts es la ejecución de estos de manera automática, mitigando en la medida de lo posible fallos ocasionados a la hora de bastionar un sistema o programa específico."

Podéis encontrar más información en los siguientes enlaces:

- Aviso del pasado 25 de marzo en el portal del CCN-CERT: https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/11661-recomendaciones-de-seguridad-de-adobe-acrobat-reader-dc.html
- Enlace al informe de buenas prácticas BP/16: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/4065-ccn-cert-bp-16-acrobat-reader-dc/file.html

Para cualquier duda o consulta al respecto, podéis contactar con nuestro equipo en ustic.stic.sspa@juntadeandalucia.es.

Gracias por la atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud